This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representation of The original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000269950 A**

(43) Date of publication of application: **29 . 09 . 00**

(51) Int. Cl **H04L 9/08**
G09C 1/00

(21) Application number: **11066405**

(22) Date of filing: **12 . 03 . 99**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

(72) Inventor: **HARADA TOSHIHARU**
TATEBAYASHI MAKOTO

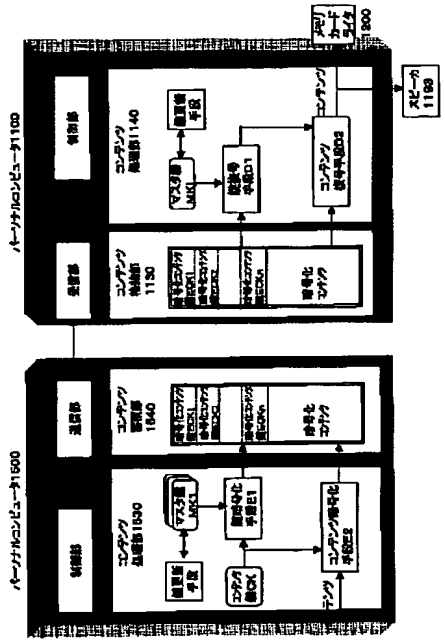
(54) **COPYRIGHT PROTECTION SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To save labor and time required for ciphering data by ciphering contents key into a ciphered contents key, ciphering contents into ciphered contents, decoding the ciphered contents key by using a master key, and updating or invalidating the master key.

SOLUTION: A contents processing part 1530, once receiving a generation indications for contents and information of the contents from a control part, generates a contents key CK and performs a ciphering process by using a key ciphering means E1 by using the contents key CK. Furthermore, the contents are ciphered by a contents ciphering means by using the contents key CK. Capsule data, as data including the ciphered contents and contents keys FEK1 to ECKn, are outputted to a contents storage part 1540. A content update device once receiving a contents update indication, the capsule data, and the master key to be invalidated invalidates the ciphered contents keys of the capsule data.

COPYRIGHT: (C)2000,JPO



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－269950
（P2000－269950A）
(43)公開日　平成12年９月29日(2000.9.29)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｄ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ	９Ａ００１
		Ｈ０４Ｌ　9/00	６０１Ｅ	

審査請求　未請求　請求項の数４　ＯＬ　（全９頁）

(21)出願番号　特願平11－66405

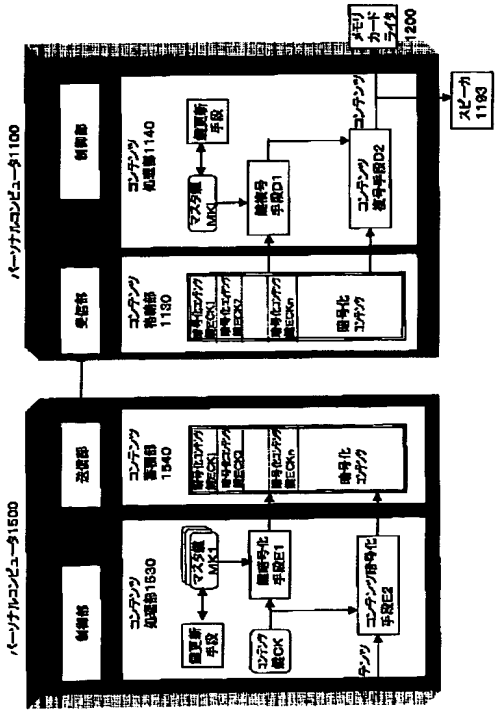
(22)出願日　平成11年３月12日(1999.3.12)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　原田　俊治
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

Ｆターム(参考)　5J104 AA01 AA13 AA16 AA34 EA06
EA18 NA02 NA37 PA14
9A001 EE03 JJ13 JJ25 LL03

(54)【発明の名称】　著作物保護システム

(57)【要約】
【課題】　著作物データ(コンテンツ)を暗号化して配布するシステムにおいて、暗号化されたコンテンツの複号に用いる鍵の盗難に対処するため、鍵を更新できるシステムを提供する。
【解決手段】　第１の装置は、第１から第ｎのマスタ鍵を用いてコンテンツ鍵を暗号化し、コンテンツ鍵を用いてコンテンツを暗号化する。第２の装置は、前記第１から第ｎのマスタ鍵のうちのいずれかである第ｊのマスタ鍵を用いて、第ｊの暗号化コンテンツ鍵を復号し、コンテンツ復号鍵を用いて、暗号化コンテンツを復号する。第ｊのマスタ鍵が盗難した場合、第1の装置及び第2の装置における第ｊのマスタ鍵を無効にするもしくは第ｎ＋１のマスタ鍵に更新する。



1

【特許請求の範囲】

【請求項１】 デジタル著作物であるコンテンツの配送システムにおける著作物保護システムであって、

第１から第ｎのマスタ鍵を用いて、コンテンツ鍵を暗号化することにより、第１から第ｎの暗号化コンテンツ鍵を作成する鍵暗号化手段と、

前記コンテンツ鍵を用いてコンテンツを暗号化することにより暗号化コンテンツを作成するコンテンツ暗号化手段と、

前記第１から第ｎのマスタ鍵のうちのいずれかである第ｊのマスタ鍵を用いて、前記第ｊの暗号化コンテンツ鍵を復号することによりコンテンツ鍵を取得する鍵復号手段と、

前記コンテンツ復号鍵を用いて、前記暗号化コンテンツを復号することによりコンテンツを取得するコンテンツ復号手段と、

前記鍵暗号化手段および前記鍵複号手段で利用される前記第ｊのマスタ鍵を無効にするもしくは前記第ｊのマスタ鍵を第ｎ＋１のマスタ鍵に更新するマスタ鍵制御手段とを備えたことを特徴とする著作物保護システム。

【請求項２】 著作物保護システムはさらに、前記鍵暗号化手段で作成された第1から第ｎの暗号化コンテンツ鍵のうち前記第ｊの暗号化コンテンツ鍵を無効にする、もしくは、前記第ｊの暗号化コンテンツ鍵を、コンテンツ鍵を第ｎ+1のマスタ鍵を用いて暗号化した結果である第ｎ＋１の暗号化コンテンツ鍵に更新する、暗号化コンテンツ鍵制御手段を備えることを特徴とする請求項１記載の著作物保護システム。

【請求項３】 前記鍵暗号化手段もしくは前記鍵複号手段は、それぞれ鍵暗号化用もしくは鍵複号用のソフトウエアを実行するパーソナルコンピュータで構成され、前記鍵制御手段により、前記第ｊのマスタ鍵を利用した前記鍵暗号化用もしくは鍵複号用のソフトウエアが、前記第ｎ＋１のマスタ鍵を利用した前記鍵暗号化用もしくは鍵複号用のソフトウエアに置き換えられることを特徴とする請求項１記載の著作物保護システム。

【請求項４】 前記鍵暗号化手段もしくは前記鍵複号手段は、それぞれ鍵暗号化もしくは鍵複号処理を実行するハードウエアで構成され、前記鍵制御手段により、前記第ｊのマスタ鍵を利用した前記鍵暗号化もしくは鍵複号処理が、前記第ｎ＋１のマスタ鍵を利用した前記鍵暗号化もしくは鍵複号処理に切り替えられることを特徴とする請求項１記載の著作物保護システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタル著作物の著作権保護を技術的に実現するためのシステムに関し、特に、ディジタル著作物たるコンテンツの再生記録における著作物保護技術に関する。

【０００２】

2

【従来の技術】近年、インターネット関連技術の発展により、音楽等のコンテンツをインターネットを通じて配送し、これをダウンロードしたユーザから料金を受け取ることも可能となってきた。

【０００３】またインターネットからパーソナルコンピュータにダウンロードされたディジタル著作物が簡単に複製できるものであるため、これを防止するために、暗号化等の技術が用いられている。

【０００４】

【発明が解決しようとする課題】ところで、このように、各種コンテンツを暗号処理して配布する場合、暗号化を行う装置に暗号鍵を持たせ、復号を行う装置に復号鍵を持たせて暗号処理して配布を行うのが一般的である。なお、ここでは、〝暗号鍵による暗号化〟という表現で、署名生成鍵による署名生成変換を、〝複号鍵による複号〟という表現で、署名検証鍵による署名検証変換処理を含む広い意味で用いている。

【０００５】しかしながら、復号鍵が盗難した場合、暗号装置及び複号装置において、盗難した復号鍵および対応する暗号鍵を無効にしたり更新するとともに、各種データに対して新しい暗号鍵で再度暗号化する必要が生じる。再度暗号化する手間は、すでに暗号化したデータの量に比例して大きくなる。

【０００６】本発明は、このような鍵更新に伴う、データの暗号処理の手間を軽減するを提供することを目的とする。

【０００７】

【課題を解決するための手段】上記目的を達成するために、本発明は、第１から第ｎのマスタ鍵を用いて、コンテンツ鍵を暗号化することにより、第１から第ｎの暗号化コンテンツ鍵を作成する鍵暗号化手段と、前記コンテンツ鍵を用いてコンテンツを暗号化することにより暗号化コンテンツを作成するコンテンツ暗号化手段と、前記第１から第ｎのマスタ鍵のうちのいずれかである第ｊのマスタ鍵を用いて、前記第ｊの暗号化コンテンツ鍵を復号することによりコンテンツ鍵を取得する鍵復号手段と、前記コンテンツ復号鍵を用いて、前記暗号化コンテンツを復号することによりコンテンツを取得するコンテンツ復号手段と、前記鍵暗号化手段および前記鍵複号手段で利用される前記第ｊのマスタ鍵を無効にするもしくは前記第ｊのマスタ鍵を第ｎ＋１のマスタ鍵に更新するマスタ鍵制御手段とを備えたことを特徴とする。

【０００８】また、著作物保護システムはさらに、前記鍵暗号化手段で作成された第１から第ｎの暗号化コンテンツ鍵のうち前記第ｊの暗号化コンテンツ鍵を無効にする、もしくは、前記第ｊの暗号化コンテンツ鍵を、コンテンツ鍵を第ｎ+1のマスタ鍵を用いて暗号化した結果である第ｎ＋１の暗号化コンテンツ鍵に更新する、暗号化コンテンツ鍵制御手段を備えることを特徴とする。

【０００９】また、前記鍵暗号化手段もしくは前記鍵複

号手段は、それぞれ鍵暗号化用もしくは鍵複号用のソフトウエアを実行するパーソナルコンピュータで構成され、前記鍵制御手段により、前記第ｊのマスタ鍵を利用した前記鍵暗号化用もしくは鍵複号用のソフトウエアが、前記第ｎ＋１のマスタ鍵を利用した前記鍵暗号化用もしくは鍵複号用のソフトウエアに置き換えられることを特徴とする。

【００１０】また、前記鍵暗号化手段もしくは前記鍵複号手段は、それぞれ鍵暗号化もしくは鍵複号処理を実行するハードウエアで構成され、前記鍵制御手段により、前記第ｊのマスタ鍵を利用した前記鍵暗号化もしくは鍵複号処理が、前記第ｎ＋１のマスタ鍵を利用した前記鍵暗号化もしくは鍵複号処理に切り替えられることを特徴とする。

【００１１】

【発明の実施の形態】以下、本発明に係わる著作物保護システムの実施の形態である音楽コンテンツ配信システムについて、図面を用いて説明する。

【００１２】＜構成＞図１は、本発明に実施の形態に係る音楽コンテンツ配信システム１０００の概観図である。

【００１３】音楽コンテンツ配信システム１０００は、パーソナルコンピュータ１５００により、音楽コンテンツを作成送信し、通信回線１００１を介して受信した音楽コンテンツをパーソナルコンピュータ１１００により再生し、また、メモリカード１３００に記録するシステムである。なお、メモリカード１３００は、厚さ数ミリ、縦横２ｃｍ四方程度の形状で、６４メガバイトの記憶容量を持ち制御回路を内臓する半導体メモリである。ユーザは、このメモリカード１３００を、メモリカード再生機器に挿入することにより、ヘッドフォーン等を通じて再生された音楽を楽しむことができる。

【００１４】パーソナルコンピュータ１５００は、CPU、メモリ、ハードディスク等を内臓し、コンテンツ提供者の指示に応じて音楽コンテンツ作成用プログラムを実行することができるものであり、通信回線１００１と接続されている。

【００１５】パーソナルコンピュータ１１００は、CPU、メモリ、ハードディスク等を内臓し、ユーザの指示に応じて音楽コンテンツ再生用プログラムを実行することができるものであり、スピーカー１１９３、及び、通信回線１００１と接続されており、また、いわゆるｐｃカードスロットであるメモリカードライタ挿入口１１９５を有する。

【００１６】メモリカードライタ１２００は、いわゆるＰＣカードであり、メモリカードを挿入するためのメモリカード挿入口１２９９を有している。

【００１７】図２は、音楽コンテンツ配信システム１０００の機能ブロック図である。

【００１８】機能的には、まず、コンテンツの提供者が利用するパーソナルコンピュータ１５００（以下提供者側ＰＣと称する）は、送信部１５１０と、制御部１５２０と、コンテンツ処理部１５３０、コンテンツ蓄積部１５４０とから構成される。ユーザが利用するパーソナルコンピュータ１１００（以下ユーザ側ＰＣと称する）は、受信部１１１０と、制御部１１２０と、コンテンツ格納部１１３０と、コンテンツ処理部１１４０とから構成される。また、スピーカ１１９３と、メモリカードライタ１２００が接続される。

【００１９】同図には、コンテンツ処理部により作成された暗号化された状態のコンテンツ（以降、カプセルデータ１００と呼ぶことにする）をも示している。カプセルデータは、通信回線からユーザが利用するパーソナルコンピュータに入力されるデータであり、音楽コンテンツとこれに関する管理情報などが暗号化されたものである。カプセルデータの内容については後程詳しく説明する。

【００２０】提供者側ＰＣ１５００における送信部１５１０と制御部１５２０と、コンテンツ処理部１５３０とは、パーソナルコンピュータ１５００のメモリに格納された音楽コンテンツ生成用プログラムが、CPUにより実行されることにより実現される機能であり、コンテンツ蓄積部１５４０は、パーソナルコンピュータ１５００のメモリ又はハードディスクの一領域である。

【００２１】音楽コンテンツ生成用プログラムは、生成する音楽コンテンツの内容をコンテンツ提供者に選択させたり、選択されたコンテンツに対する課金条件を受け付けるためのものであり、制御部１５２０は、キーボードによる提供者の操作を受け付け、これに応じて、音楽コンテンツの生成を行うものである。

【００２２】コンテンツ処理部１５３０は、制御部１５２０からのコンテンツの生成指示と、コンテンツの情報を受け取ると、コンテンツ鍵ＣＫを生成し、このコンテンツ鍵ＣＫを、n個のマスタ鍵ＭＫ１、…、ＭＫnを用いて、それぞれ鍵暗号化手段にて暗号化処理Ｅ１を行い、また、コンテンツＣＯを、コンテンツ鍵ＣＫを用いてコンテンツ暗号化手段にて暗号化処理Ｅ２を行う。すなわち、暗号化コンテンツ鍵ＥＣＫｉ＝Ｅ１（ＭＫｉ、ＣＫ）（ｉ＝１，２、…、ｎ）暗号化コンテンツ　ＥＣＯ＝Ｅ２（ＣＫ、ＣＯ）である。ここで、mを、鍵ｋで暗号化処理Ｅで暗号化した結果がｃであるとき、ｃ＝Ｅ（ｋ、ｍ）と記す。そして、暗号化したコンテンツＥＣＯと、暗号化したn個のコンテンツ鍵ＥＣＫ１、…、ＥＣＫｎを含むデータであるカプセルデータをコンテンツ蓄積部に出力する。

【００２３】送信部１５１０は、制御部１５２０からの送信指示を受けて、インターネットに接続された通信回線１００１に、コンテンツ蓄積部１５４０に格納されたカプセルデータを送信する。

【００２４】ユーザ側ＰＣ１１００における受信部１１

１０と制御部１１２０と、コンテンツ処理部１１３０とは、パーソナルコンピュータ１１００のメモリに格納された音楽コンテンツ再生用プログラムが、CPUにより実行されることにより実現される機能であり、コンテンツ蓄積部１５５０は、パーソナルコンピュータ１５００のメモリ又はハードディスクの一領域である。

【００２５】音楽コンテンツ再生用プログラムは、受信すべき音楽コンテンツをユーザに選択させたり、選択された音楽コンテンツを再生するか、記録するか等のユーザの指示を受け付けるためのものであり、制御部１１２０は、キーボードによる提供者の操作を受け付け、これに応じて、音楽コンテンツの受信指示、再生指示、記録指示等を行うものである。

【００２６】受信部１１１０は、制御部１１２０からの受信指示を受けて、インターネットに接続された通信回線１００１からカプセルデータを受信して、コンテンツ格納部１１３０に格納し、格納場所を制御部１１２０に通知する。

【００２７】コンテンツ処理部１１４０は、制御部１１２０から、再生もしくは記録指示とカプセルデータの格納場所についての情報とを受け取ると、まず、第ｊのマスタ鍵を用いて、暗号化されたｎ個のコンテンツ鍵ＥＣＫｉ（ｉ＝１，２、…、ｎ）の中の第ｊの暗号化したコンテンツ鍵ＥＣＫｊを、鍵復号手段にて復号処理Ｄ１を用いて復号し、復号したコンテンツ鍵ＣＫを用いて、暗号化されたコンテンツＥＣＯをコンテンツ復号手段にて復号処理Ｄ２を用いて復号する。

【００２８】すなわち、

ＣＫ＝Ｄ１（ＭＫｊ、ＥＣＫｊ）

ＣＯ＝Ｄ２（ＣＫ、ＥＣＯ）

である。ここで、ｃを、鍵ｋで復号処理Ｄで復号した結果がｍであるとき、ｍ＝Ｄ（ｋ、ｃ）と記す。

【００２９】復号したコンテンツを、再生指示の場合スピーカに出力し、記録指示の場合、メモリカードライタに出力し、図示していないが、メディアカードライタは、コンテンツを暗号化した上で、メディアカードへ記録する。

【００３０】＜データ構造と関連処理＞提供者側ＰＣ1500に入力されるコンテンツは、音楽データ、歌詞などのテキストデータ、ビデオクリップなど画像データより構成される。

【００３１】図３は、暗号化コンテンツＥＣＯ生成過程を示すデータフロー図である。同図に示すように、暗号化コンテンツＥＣＯは、平文であるコンテンツＣＯを、コンテンツ鍵ＣＫで暗号化することにより生成されるデータである。ＣＫは５６ビットの鍵データであり、暗号化はブロック暗号方式で行い、例えばＤＥＳ（ＤａｔａＥｎｃｒｙｐｔｉｏｎＳｔａｎｄａｒｄ）アルゴリズムが用いられる。

【００３２】なお暗号化の際、コンテンツは、６４ビット毎のデータブロックに分割され、分割されたデータブロックがそれぞれ、５６ビットのコンテンツ鍵ＣＫを用いて暗号化され、６４ビットの暗号化されたデータブロックが生成される。こうして得られる６４ビットの暗号化された各データブロックは結合され、暗号化コンテンツとして出力される。

【００３３】また５６ビットのコンテンツ鍵ＣＫは、コンテンツ処理部において、例えば各コンテンツ毎に固有に生成される。

【００３４】図４は、暗号化コンテンツ鍵ＥＣＫｉの生成過程を示すデータフロー図である。同図に示すように、暗号化コンテンツ鍵ＥＣＫｉは、コンテンツ鍵ＣＫを、マスタ鍵ＭＫｉで暗号化することにより生成されるデータである。ＭＫｉは、例えば112ビットの鍵データであり、暗号化は公開鍵暗号方式の１種である楕円曲線暗号アルゴリズムが用いられる。このとき、提供者側ＰＣのコンテンツ処理部では、マスタ鍵ＭＫｉとして、楕円秘密鍵もしくは楕円公開鍵のうちのどちらか用い、利用者側ＰＣのコンテンツ処理部では、マスタ鍵ＭＫｉとして、対応する楕円公開鍵、もしくは対応する楕円秘密鍵のうちのどちらか一方を用いる。

【００３５】なお、楕円暗号については、ＤｏｕｇｌａｓＲ．Ｓｔｒｉｎｓｏｎ著「暗号理論の基礎」（共立出版株式会社）に詳細に説明されている。

【００３６】なお、同図では示していないが、コンテンツ鍵に管理情報を含めて同様に暗号化してもよい。

【００３７】ここで、管理情報は、コンテンツに関連した情報であり、コンテンツの復号条件情報、課金情報を含む。復号条件情報は、コンテンツを復号する条件を示す情報であり、復号することを許容する期日、回数などを示す情報である。また課金情報は、コンテンツを復号する際に請求されるべき料金に関する情報、即ち、音楽コンテンツの使用料金や購入料金を示す情報である。

【００３８】＜鍵更新時の処理＞ユーザ側ＰＣのマスタ鍵ＭＫｊが、何らかの理由で暴露され更新する必要が生じた場合に対応するため、ユーザ側ＰＣのコンテンツ処理部１５３０は、制御部１５２０から、鍵更新指示と、無効にすべきマスタ鍵ＭＫｊ、および、オプションとして新しいマスタ鍵ＭＫＮ＋１を受け取ると、鍵暗号化手段において用いるマスタ鍵ＭＫ１、ＭＫ２、…、ＭＫｎのうち、ＭＫｊの使用を中止するとともに、オプションとして新しいマスタ鍵ＭＫＮ＋１を受け取った場合は、鍵暗号化手段においてＭＫｎ＋１をあたらに使用するようにすることもできるものである。

【００３９】また、提供者側ＰＣのコンテンツ処理部１１３０は、制御部１１２０から、鍵更新指示と、無効にすべきマスタ鍵ＭＫｊ、および、オプションとして新しいマスタ鍵ＭＫＮ＋１を受け取ると、鍵暗号化手段において用いるＭＫｊの使用を中止するとともに、オプションとして新しいマスタ鍵ＭＫＮ＋１を受け取った場合

は、鍵暗号化手段においてＭＫｎ＋１をあたらに使用するようにする。

【００４０】以上の構成により、鍵更新された提供者側ＰＣで生成されるカプセルデータは、鍵更新されたユーザ側ＰＣを用いてしか、再生記録できないようにすることができ、これによりユーザＰＣ側のマスタ鍵の暴露への対処が可能となる。

【００４１】また、図５に、コンテンツ更新装置の構成を示す。

【００４２】同図に示すようにコンテンツ更新装置１６００は、CPU、メモリ、ハードディスク等を内臓し、コンテンツ提供者の指示に応じて音楽コンテンツ更新用プログラムを実行することができるものであり、提供者側ＰＣ１５００と接続されている。あるいは、提供者側ＰＣ１５００そのものであってもよい。

【００４３】コンテンツ更新装置は、制御部１６１０と、コンテンツ処理部１６２０とから構成される。制御部から、コンテンツ更新指示と、カプセルデータと、無効にすべきマスタ鍵ＭＫｊを受け取ると、カプセルデータにおける暗号化コンテンツ鍵ＣＫｊを無効にするものである。

【００４４】以上の構成により、鍵更新前に提供者側ＰＣで生成されるカプセルデータにつても、鍵更新されたユーザ側ＰＣを用いてしか、再生記録できないようにすることができ、これによりユーザＰＣ側のマスタ鍵の暴露への対処が可能となる。

【００４５】以上、本発明に係わる著作物保護システムについて、実施の形態である音楽コンテンツ配信システムに基づいて説明したが、本発明はこれらの実施の形態にかぎられないことは勿論である。即ち、

（１）本実施の形態では、送信部１５１０、制御部１５２０、コンテンツ処理部１５３０、コンテンツ蓄積部１５４０は、パーソナルコンピュータ１５００により実現されるものとしたが、パーソナルコンピュータ１５００は、メモリ及びＣＰＵを備えプログラム実行制御機能を有する機器であればよく、また、受信部１１１０、制御部１１２０、コンテンツ処理部１１４０、コンテンツ格納部１１３０、はパーソナルコンピュータ１１００により実現されるものとしたが、パーソナルコンピュータ１１００は、メモリ及びＣＰＵを備えプログラム実行制御機能を有する家電機器であればよく、例えば、インターネット接続機能をもつテレビ受信機であってもよい。

【００４６】また、本実施の形態における、メモリカードに音楽データを記録するメモリカードライタは、ＰＣカードであるとしたが、これに限定されることはなく、パーソナルコンピュータと接続可能な機器であればよく、例えばＵＳＢ（ＵｎｉｖｅｒｓａｌＳｅｒｉａｌＢｕｓ）等により接続される機器であればよい。

【００４７】（２）本実施の形態では、コンテンツ鍵が５６ビット、マスタ鍵が１１２ビット等と、鍵データについて長さを示したが、この長さに限定されることはない。また本実施例における暗号アルゴリズムもＤＥＳや楕円曲線暗号に限定されることはない。

【００４８】（３）本実施の形態では、カプセルデータは、通信回線を通じて送られるものとしたが、これに限定されることはなく、例えば、光ディスクなどの記録媒体に格納されるものであってもよい。この場合、送信部1510は、カプセルデータを記録媒体に記録するようにし、受信部1110は、カプセルを記録媒体から読み出しコンテンツ格納部に格納するようなものであればよい。

【００４９】（４）本実施の形態では、メモリカードライタを用いてメモリカードに記録するものとしたが、これに限定されることはなく、例えば、光ディスク記録ドライブを用いて光ディスク等の記録媒体に記録するものとしてもよい。

【００５０】（５）本実施の形態では、コンテンツを暗号化するものとしたが、コンテンツの一部を暗号化するものとしてもよい。

【００５１】（６）本実施の形態では、提供者側ＰＣにおいてあらかじめ複数のマスタ鍵を保持している構成としたが、これに限定されることはなく、単数であってもよい。

【００５２】また、提供者側ＰＣ装置におけるコンテンツ生成プログラム、及び、ユーザ側ＰＣ装置におけるコンテンツ再生プログラムは及びパーソナルコンピュータを介して外部ネットワークからダウンロードできるようにしてもよく、マスタ鍵の更新されたプログラムをダウンロードして利用することにより、マスタ鍵の更新を実現してもよい。また特定のマスタ鍵を削除する機能を有するものであってもよい。またマスタ鍵を取り込む際、署名情報を確認し、正当な場合のみマスタ鍵を取り込むこととしてもよい。

【００５３】また、提供者側ＰＣ装置におけるコンテンツ生成プログラム、及び、ユーザ側ＰＣ装置におけるコンテンツ再生プログラムを実行するためのマスタ鍵などのデータ、もしくは、プログラムを、各ＰＣ装置に着脱可能なハードウエアにおいて実行するようにしてもよく、鍵の更新されたハードウエアをＰＣに装着することにより、鍵更新を実現してもよい。

【００５４】

【発明の効果】以上の説明から明らかなように、本発明に係わる著作物保護システムは、デジタル著作物であるコンテンツの配送システムにおける著作物保護システムであって、第１から第ｎのマスタ鍵を用いて、コンテンツ鍵を暗号化することにより、第１から第ｎの暗号化コンテンツ鍵を作成する鍵暗号化手段と、前記コンテンツ鍵を用いてコンテンツを暗号化することにより暗号化コンテンツを作成するコンテンツ暗号化手段と、前記第１から第ｎのマスタ鍵のうちのいずれかである第ｊのマスタ鍵を用いて、前記第ｊの暗号化コンテンツ鍵を復号す

ることによりコンテンツ鍵を取得する鍵復号手段と、前記コンテンツ復号鍵を用いて、前記暗号化コンテンツを復号することによりコンテンツを取得するコンテンツ復号手段と、前記鍵暗号化手段および前記鍵複号手段で利用される前記第ｊのマスタ鍵を無効にするもしくは前記第ｊのマスタ鍵を第ｎ＋１のマスタ鍵に更新するマスタ鍵制御手段とを備えたことを特徴とする。

【００５５】これにより、鍵更新された提供者側ＰＣで生成されるカプセルデータは、鍵更新されたユーザ側ＰＣを用いてしか、再生記録できないようにすることができ、これによりユーザＰＣ側のマスタ鍵の暴露への対処が可能となる。

【００５６】また、著作物保護システムはさらに、前記鍵暗号化手段で作成された第1から第ｎの暗号化コンテンツ鍵のうち前記第ｊの暗号化コンテンツ鍵を無効にする、もしくは、前記第ｊの暗号化コンテンツ鍵を、コンテンツ鍵を第ｎ+1のマスタ鍵を用いて暗号化した結果である第ｎ＋１の暗号化コンテンツ鍵に更新する、暗号化コンテンツ鍵制御手段を備えることとすることもできる。

【００５７】これににより、鍵更新前に提供者側ＰＣで生成されるカプセルデータにつても、鍵更新されたユーザ側ＰＣを用いてしか、再生記録できないようにすることができ、これによりユーザＰＣ側のマスタ鍵の暴露への対処が可能となる。

【００５８】また、前記鍵暗号化手段もしくは前記鍵複号手段は、それぞれ鍵暗号化用もしくは鍵複号用のソフトウエアを実行するパーソナルコンピュータで構成さ＊れ、前記鍵制御手段により、前記第ｊのマスタ鍵を利用した前記鍵暗号化用もしくは鍵複号用のソフトウエアが、前記第ｎ＋１のマスタ鍵を利用した前記鍵暗号化用もしくは鍵複号用のソフトウエアに置き換えられることとすることもできる。

【００５９】これにより、ソフトウエアのダウンロードにより、盗難などで暴露された鍵を無効にするとともに、新しい鍵に更新することが可能となる。

【００６０】また前記鍵暗号化手段もしくは前記鍵複号手段は、それぞれ鍵暗号化もしくは鍵複号処理を実行するハードウエアで構成され、前記鍵制御手段により、前記第ｊのマスタ鍵を利用した前記鍵暗号化もしくは鍵複号処理が、前記第ｎ＋１のマスタ鍵を利用した前記鍵暗号化もしくは鍵複号処理に切り替えられることとすることもできる。

【００６１】これにより、ハードウエアの交換により、盗難などで暴露された鍵を無効にするとともに、新しい鍵に更新することが可能となる。

【図面の簡単な説明】

【図１】本発明に係る著作物保護システムの実施の形態である音楽コンテンツ再生記録システムの概観図

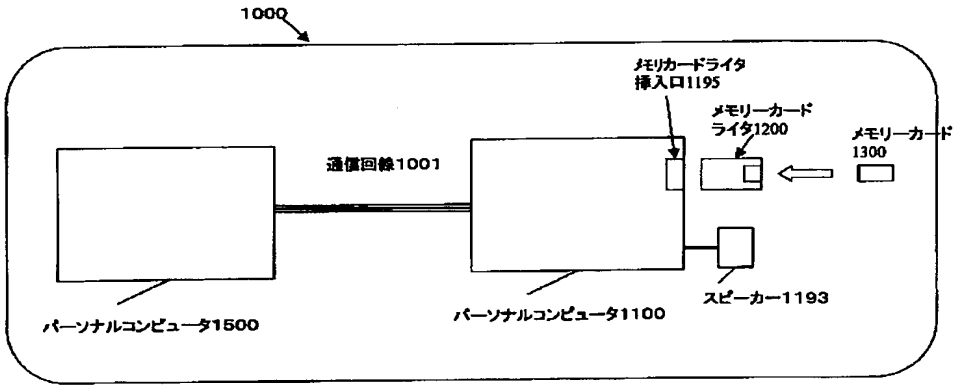
【図２】音楽コンテンツ配信システムの機能ブロック図

【図３】暗号化コンテンツ、及び、暗号化コンテンツ鍵の生成過程を示すデータフロー図

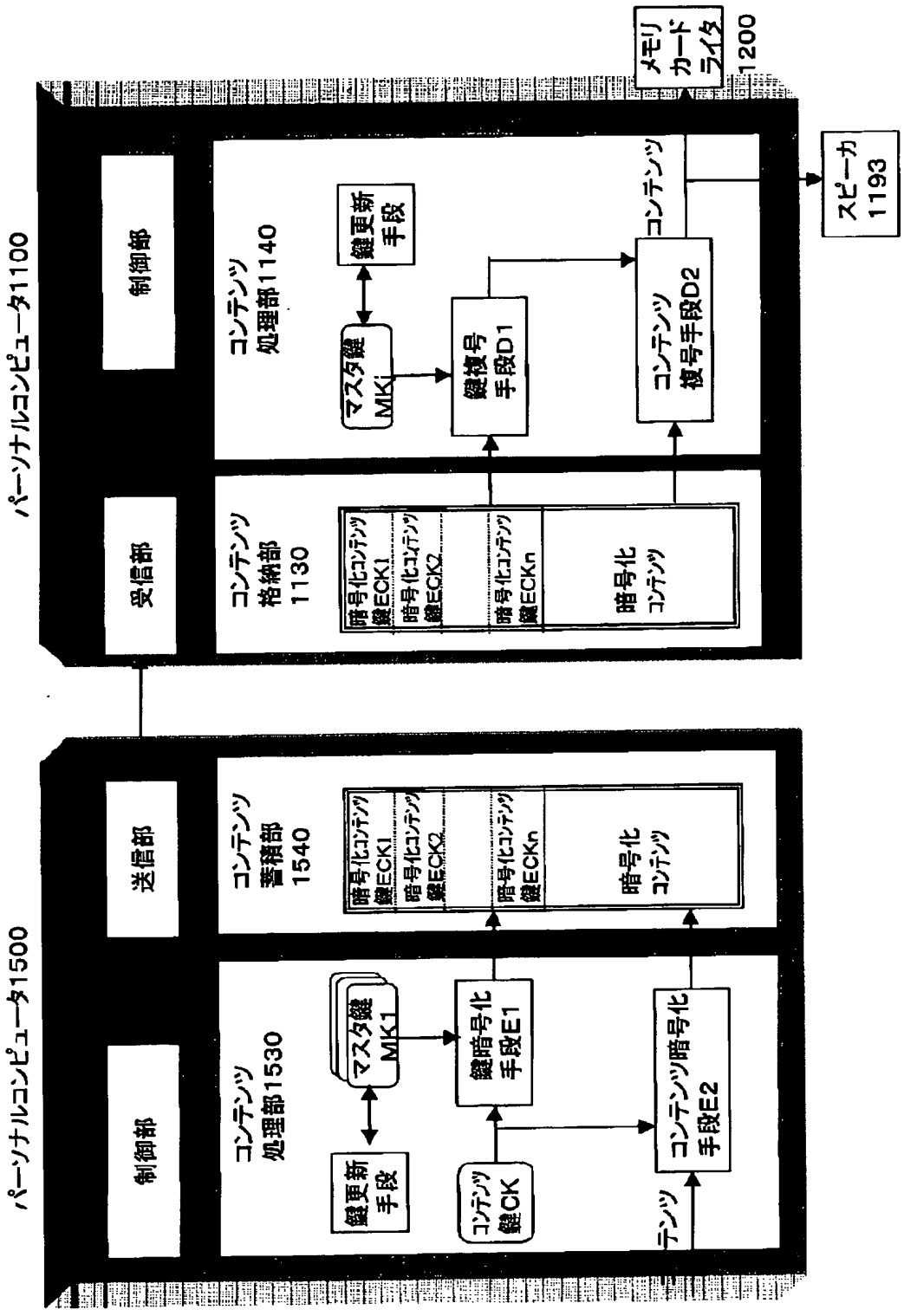
【図４】暗号化コンテンツ鍵ＥＣＫｉの生成過程を示すデータフロー図

【図５】コンテンツ更新装置の機能ブロック図

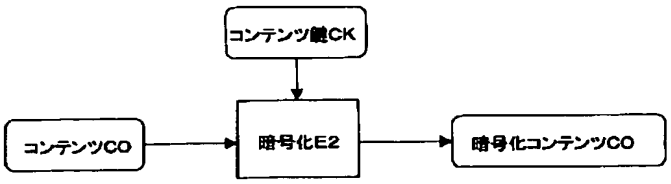
【図１】



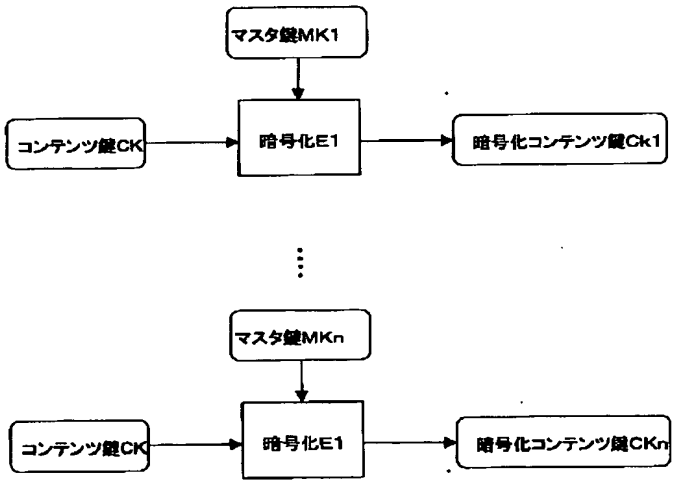
【図２】


パーソナルコンピュータ1500
制御部
送信部
コンテンツ
処理部1530
マスタ鍵
MKi
鍵更新
手段
鍵暗号化
手段E1
コンテンツ
鍵CK
コンテンツ暗号化
手段E2
コンテンツ
蓄積部
1540
暗号化コンテンツ
鍵ECK1
暗号化コンテンツ
鍵ECK2
暗号化コンテンツ
鍵ECKn
暗号化
コンテンツ
パーソナルコンピュータ1100
制御部
受信部
コンテンツ
処理部1140
マスタ鍵
MKi
鍵更新
手段
鍵複号
手段D1
コンテンツ
複号手段D2
コンテンツ
コンテンツ
格納部
1130
暗号化コンテンツ
鍵ECK1
暗号化コンテンツ
鍵ECK2
暗号化コンテンツ
鍵ECKn
暗号化
コンテンツ
メモリ
カード
ライタ
1200
スピーカ
1193

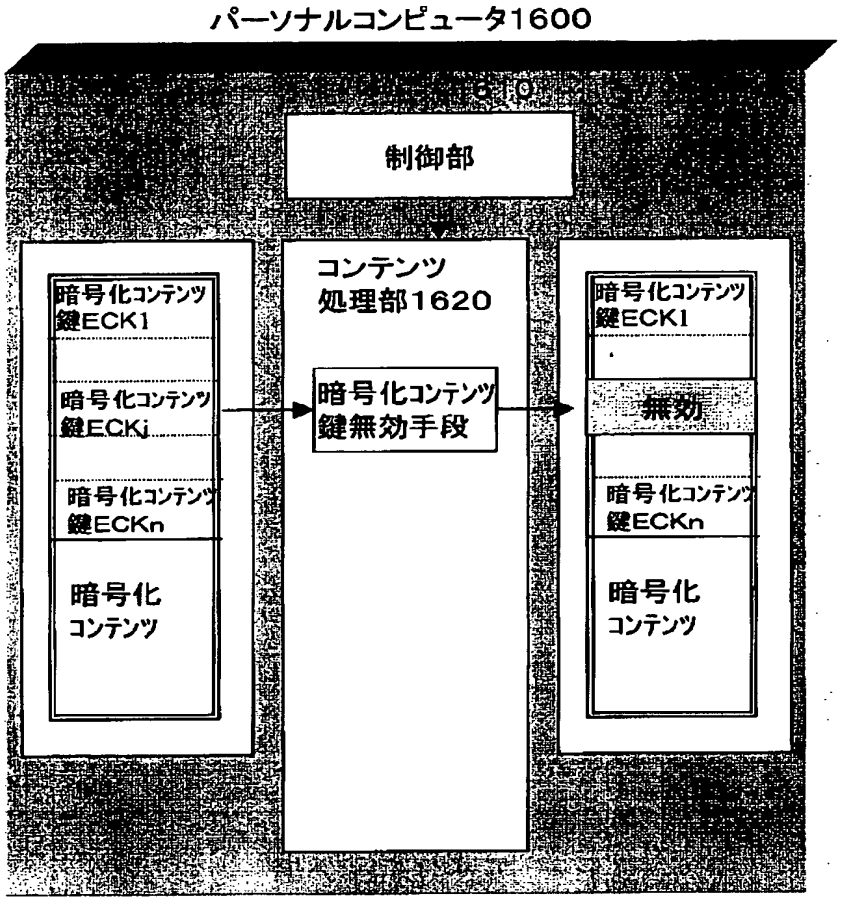
【図３】


コンテンツ鍵CK
コンテンツCO
暗号化E2
暗号化コンテンツCO

【図４】


マスタ鍵MK1
コンテンツ鍵CK
暗号化E1
暗号化コンテンツ鍵Ck1
マスタ鍵MKn
コンテンツ鍵CK
暗号化E1
暗号化コンテンツ鍵CKn

【図５】


パーソナルコンピュータ1600
I/O
制御部
コンテンツ
処理部1620
暗号化コンテンツ
鍵ECK1
暗号化コンテンツ
鍵ECKi
暗号化コンテンツ
鍵ECKn
暗号化
コンテンツ
暗号化コンテンツ
鍵無効手段
暗号化コンテンツ
鍵ECK1
無効
暗号化コンテンツ
鍵ECKn
暗号化
コンテンツ